四次アーベル体の整数環の巾底について (実験整数論)

AUTHOR(S):

中原, 徹

CITATION:

中原, 徹. 四次アーベル体の整数環の巾底について (実験整数論). 数理解析研究所講究録 1979, 371: 31-46

ISSUE DATE:

1979-12

URL:

http://hdl.handle.net/2433/104689

数理解析研究所講究録
371巻 1979年 31-46

四次アーベル体の整数環の巾底について

佐賀大 理工 中原 徹

§1. 序

K を有理数体 $\mathbb{Q}$ 上の次数 n の有限次アーベル拡大体，$\mathcal{O}_K$ をその整数環とする．$\mathcal{O}_K$ は整数の組 $\{\omega_1, \cdots, \omega_n\}$ を基底にもつ有理整数環 $\mathbb{Z}$ 上の自由加群 $\mathbb{Z}[\omega_1, \cdots, \omega_n]$ である．K が円周等分体またはその最大実部分体のとき，二次体と同じく例外なしに $\mathcal{O}_K$ の基底は適当な整数 α の巾で採れることがわかっている [5], [6]．以後 K において $\mathcal{O}_K = \mathbb{Z}[1, \alpha, \cdots, \alpha^{n-1}]$ が成り立つとき $\mathcal{O}_K$ は巾底 (power basis) をもつという．

問題．整数環が巾底をもつ有限次アーベル体を特徴づけよ．

本稿の目的は $K/\mathbb{Q}$ が四次アーベル拡大の場合を調べることである．

一般に，K の任意の整数 α について $1, \alpha, \cdots, \alpha^{n-1}$ の基底 $\{\omega_1, \cdots, \omega_n\}$ による表現行列を (a_{jk}) とおけば数 α の判別式 $d(\alpha)$ と体 K の判別式 $d(K)$ との間に $d(\alpha) = \det(a_{jk})^2 d(K)$ が成り立つ．もしも α が $\mathbb{Q}$ 上 K の原始要素ならば $|\det(a_{jk})|$ は

群指数 $(\mathcal{O}_K : \mathbb{Z}[1, \alpha, \cdots, \alpha^{n-1}])$ に等しい．α がそうでないとき $\det(a_{jk}) = 0$ となる．よってわれわれは非負整数 $|\det(a_{jk})|$ を $Ind\,\alpha$ と書き，α の判別式の仮因子という．このとき，それらの最大公約数 $g.c.d._{\alpha \in \mathcal{O}_K}\{Ind\,\alpha\}$ は K によって決まる不変量の一つであるから体 K の判別式の仮因子と定義される．これを $\mathfrak{d}(K)$ と書く．Mensel によれば「n 次の代数体 K について素数 p が $\mathfrak{d}(K)$ の約数であるための一つの必要十分条件は p の K での素イデアル分解を $p \cong \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_k^{e_k}$ とするときある f に対し p の分解にあらわれる f 次の素イデアル $\mathfrak{p}_j$ の個数 λ_f が mod.p での f 次の既約多項式の個数より多い，すなわち $\lambda_f > \frac{1}{f}\sum_{d|f} \mu(d) p^{\frac{f}{d}}$ が成り立つこと」である．ここに $\mu(\cdot)$ は möbius の関数をあらわす．さらに $p | \mathfrak{d}(K)$ ならば，素数 p は体次数 n よりも小さいことが知られている．また，p が K で完全分解するならば逆も正しい[10].

D. S. Dummit と H. Kisilevsky は整数環が中底をもつ無限に多くのある種の三次巡回体を発見した[1]．体 K の判別式の仮因子 $\mathfrak{d}(K)$ が生じないときは $\mathcal{O}_K$ は中底をもつかどうか一般には判定できないけれども，もしもそれが存在すれば $\mathcal{O}_K$ は中底をもちえない．K が四次体のとき $\mathfrak{d}(K)$ の素因数は 2 または 3 に限られる．

周知のように任意の有限次アーベル拡大体 K はある円周 n

等分体K_nの部分体である（たとえば[9]）．§2ではKとしてある円分体K_nの部分体を動かすことにより仮因子分(K)が偶数となる四次巡回体を無限に多く構成する．このとき四次剰余指標χに付随したGaussの和およびGaussの四次剰余の相互法則とが本質的である．§3では最近探査された整数環が巾底をもつ四次巡回体の例を述べる．一方，Kが非巡回，アーベル四次体のとき，その整数環が巾底をもつ現象は最後の§で見出される．

§2. 四次巡回体の判別式の仮因子

自然数$n=\prod_{j=1}^{\tau} p_j$，各p_jは mod. 4 で1と合同な互いに相異なる素数，に対し円周n等分体K_nの有理数体Q上のガロア群G_nは mod. n の既約剰余類群$G=\{x \bmod n\,;\,(x,n)=1\}$に同型である．$\mathfrak{X}$をアーベル群Gの指標群，$p_j=\pi_j\bar{\pi}_j$をGaussの数体での素因数分解とする．ここに$\bar{\alpha}$は数$\alpha$の複素共役数をあらわし$\pi_j$は$\pi_j\equiv 1 \bmod (1-i)^3$と正規化しておく．ただし$i=\sqrt{-1}$である．以後，類$x \bmod n$の代表数xをGの元とみなす．Gの元xについて四次剰余記号$\left(\frac{x}{\pi_j}\right)_4$または一般Euler規準で定まる導手$p_j$の純四次指標を$\chi_j$ $(1\leqq j\leqq \tau)$とおく．すなわち

$$\chi_j(x)=\left(\frac{x}{\pi_j}\right)_4\equiv x^{\frac{p-1}{4}} \bmod \pi_j$$

が成り立つ．このとき$\chi=\prod_{j=1}^{\tau}\chi_j$とおけば$\chi$は導手nの純四次

指標となる．χで生成されるGの部分群$\langle\chi\rangle$は位数4をもつ．いま $H=\{x\in G;\ \langle\chi\rangle$の任意の元$\chi'$に対し$\chi'(x)=1\}$ とおけばHはGの部分群で，剰余群G/Hは位数4の巡回群である．Kを群Hで固定されるK_nの部分体とせよ．このとき拡大K/Qは$G/H=\langle\sigma H\rangle$に同型なガロア群をもつ四次巡回拡大である．以下$G$の元をガロア群$\mathfrak{G}$の元とみなす．さて，1の一つの原始$n$乗根$\zeta$に対し

$$\eta=\sum_{S\in H}\zeta^{S}$$

とおけばηは$\mathfrak{G}_{aus}$の$\varphi(n)/4$項周期である．ここに$\varphi(\cdot)$はEulerの関数をあらわす．$\eta^{(j)}=\eta^{\sigma^j}$, $j \bmod 4$ とおけばη, η', η'', η'''はQ上一次独立であるから$K=Q(\eta)$が成り立つ．

補題1．$\mathfrak{G}_{aus}$の$\varphi(n)/4$項周期とそのQ上の共役数$\eta, \eta', \eta'', \eta'''$は$K$の整数環$O_K$の整数基底をつくる．

証明．$O_K\subseteq Z[\eta,\eta',\eta'',\eta''']$を示せば十分である．$O_K$の任意の数$\alpha$について $\alpha=\sum_{j=0}^{3}(a_j/b_j)\eta^{(j)}$ なる有理数a_j/b_j, $(a_j,b_j)=1$が一意的に決まる．一方，αはK_nの整数であるから $\alpha=\sum_{k \bmod \varphi(n)} c_k\zeta^k$, $c_k\in Z$ と表される．最小公倍数 $l.c.m\{b_j\}$ をbとおけば $b\alpha=\sum_{j=0}^{3}(b/b_j)a_j\eta^{(j)}=\sum_{j=0}^{3}\sum_{S\in H}(b/b_j)a_j\zeta^{S\sigma^j}$ $\left(0\le j\le 3\right)$ となる．他方，$b\alpha=\sum_{k \bmod \varphi(n)} bc_k\zeta^k$ との係数を比較すれば任意のjについて $(b/b_j)a_j\equiv 0 \bmod b$が成り立つ．$\therefore a_j\equiv 0 \bmod b_j$ ところが

$(a_j, b_j)=1$ より $b_j=\pm 1$ が必要である. $\therefore \alpha=\sum_{j=0}^{3}\pm a_j\eta^{(j)}$ をえる.
これで補題の証明はできた.

注意1. $\eta, \eta', \eta'', \eta'''$ の中で一つを1とおきかえられるから、O_k の基底が1を含むようにできる.

次にわれわれは η を根にもつ四次巡回方程式 $f(X)$ を求めなければならない. n が素数 p の場合, すなわち $Q(\eta)$ が素円体 k_p の部分体のとき $f(X)$ を explicit に求める L. E. Dickson の方法があり, これは k_n が必ずしも素円体でない場合に拡張された [11]. これらの方法は具体的な例を10進15桁前後の数値実験で探査するために有効な一つの理論であり, 論文[11]のある種の一般化を示唆するものであった. 実際, 一般的には三次巡回方程式の決定[3],[8]についての analogue を考える.

先の指標 χ に付随した Gauss の和を

$$\tau(\chi)=\sum_{x\in G}\chi(x)\zeta^x$$

とおく. このとき $\chi(x)$ の値でくくり直せば

$$\tau(\chi)=\sum_{\sigma H\in G/H}\chi(\sigma)\eta^{\sigma}$$

をえる. すなわち

$$\tau(\chi)=\eta+i\eta'+i^2\eta''+i^3\eta'''$$
$$\tau(\chi^2)=\eta+i^2\eta'+\eta''+i^2\eta'''$$
$$\tau(\bar{\chi})=\eta+i^3\eta'+i^2\eta''+i\eta'''$$

が成り立つ．ここに $\bar{\chi}$ は χ の共役指標：$\bar{\chi}(x)=\overline{\chi(x)}$ を意味する．

$\eta+\eta'+\eta''+\eta'''=(-1)^2$ に注意すれば

$$\eta=\frac{1}{4}\{\tau(\chi)+\tau(\chi^3)+\tau(\bar{\chi})+(-1)^2\}$$
$$\eta'=\frac{1}{4}\{i^3\tau(\chi)+i^2\tau(\chi^3)+i\tau(\bar{\chi})+(-1)^2\}$$
$$\eta''=\frac{1}{4}\{i^2\tau(\chi)+\tau(\chi^3)+i^2\tau(\bar{\chi})+(-1)^2\}$$
$$\eta'''=\frac{1}{4}\{i\tau(\chi)+i^2\tau(\chi^3)+i^3\tau(\bar{\chi})+(-1)^2\}$$

となる．従って

$$\eta\eta'+\eta\eta''+\eta\eta'''+\eta'\eta''+\eta'\eta'''+\eta''\eta'''$$
$$=\frac{1}{16}\{-4\tau(\chi)\tau(\bar{\chi})-2\tau(\chi^2)^2+6\},$$

$$\eta\eta'\eta''+\eta\eta'\eta'''+\eta\eta''\eta'''+\eta'\eta''\eta'''$$
$$=\frac{1}{64}\left[4\{\tau(\chi)^2\tau(\chi^3)+\tau(\bar{\chi})^2\tau(\bar{\chi}^3)\}+(-1)^2 2\{-4\tau(\chi)\tau(\bar{\chi})-2\tau(\chi^2)^2\}+4(-1)^2\right],$$

$$\eta\eta'\eta''\eta'''$$
$$=\frac{1}{256}\left[-\{\tau(\chi)^4+\tau(\bar{\chi})^4\}+\tau(\chi^2)^4+2\tau(\chi)^2\tau(\bar{\chi})^2-4\tau(\chi)\tau(\bar{\chi})\tau(\chi^2)^2\right.$$
$$\left.+(-1)^2 4\{\tau(\chi)^2\tau(\chi^3)+\tau(\bar{\chi})^2\tau(\bar{\chi}^3)\}+\{-4\tau(\chi)\tau(\bar{\chi})-2\tau(\chi^2)^2\}+1\right]$$

をえる．χ^2 は導手 n の二次指標となるので

$$\tau(\chi^2)=\sqrt{\chi^2(-1)n}=\sqrt{(-1)^{\frac{n-1}{2}}n}=\sqrt{n}$$

が従う．いまとくに，$n=a^2+16$，$a\equiv 1 \bmod 4$ とおく．さらに n が平方因数を含まないとすれば n の任意の素因数 p_j について平方剰余の相互法則から $p_j\equiv 1 \bmod 4$ である．よって適当に素元 π_j を選べば $\pi=\prod_{j=1}^{2}\pi_j$ に対し $n=\pi\cdot\bar{\pi}$，$\pi=a+4i$ $\equiv 1 \bmod (1-i)^3$ となるようにできる．このとき Gauss の四次剰余

の相互法則の補充法則を用いて $\chi(-1)=\left(\frac{i}{\pi}\right)_4^2=\left(i^{\pm\frac{q-1}{2}}\right)^2=1$

をえる[4]. よって Gauss の和のノルム関係

$$\tau(\chi)\tau(\overline{\chi})=\tau(\chi)\chi(-1)\overline{\tau(\chi)}=\tau(\chi)\overline{\tau(\chi)}=\pi$$

および $\tau(\chi)^2\tau(\chi^2)=\frac{\tau(\chi)^2}{\tau(\chi^2)}\tau(\chi^2)^2=(-1)^2\chi(-1)\pi(\sqrt{\pi})^2=(-1)^2\pi\pi$

が従う[2],[3]. ここに $\frac{\tau(\chi)^2}{\tau(\chi^2)}$ は指標 χ に付随した Jacobi の和である. さらに $\tau(\chi)^4=\pi^2\pi$ が成り立つ. 従って η を根にもつ Q 上既約な四次方程式は $\pi=\prod_{j=1}^{2}\beta_j$, $\beta_j\neq\beta_k\ (j\neq k)$ に対し

$$f(X)=X^4-(-1)^2X^3+\frac{3}{8}(-\pi+1)X^2-\frac{(-1)^2}{16}\{(2a-3)\pi+1\}X$$
$$+\frac{1}{256}\{-3\pi^2+(8a+58)\pi+1\}=0$$

となる. 次に $f'(x)$ を多項式 $f(x)$ の微分とする. このとき $f'(\eta)$ の $1,\eta,\eta^2,\eta^3$ による表現行列を (b_{jk}), $b_{jk}\in\mathbb{Z}$ とおけば

$$\begin{pmatrix}1&1&1&1\\ \eta&\eta'&\eta''&\eta'''\\ \eta^2&\eta'^2&\eta''^2&\eta'''^2\\ \eta^3&\eta'^3&\eta''^3&\eta'''^3\end{pmatrix}\begin{pmatrix}f'(\eta)&&&0\\ &f'(\eta')&&\\ &&f'(\eta'')&\\ 0&&&f'(\eta''')\end{pmatrix}=\begin{pmatrix}&&&\\ &b_{jk}&&\\ &&&\\ &&&\end{pmatrix}\begin{pmatrix}1&1&1&1\\ \eta&\eta'&\eta''&\eta'''\\ \eta^2&\eta'^2&\eta''^2&\eta'''^2\\ \eta^3&\eta'^3&\eta''^3&\eta'''^3\end{pmatrix}$$

であるから η の判別式 $d(\eta)$ は $d(\eta)=N_{K/Q}f'(\eta)=\det(b_{jk})$ により行列式 $\det(b_{jk})$ を計算すればよい. ここに $N_{K/Q}$ は K/Q に関するノルムを意味する. これより

$$d(\eta)=2^2\pi^3$$

をえる.

他方, 体 K の判別式 $d(K)$ は Hasse の導手判別公式を用いれ

ば $f(x)$ を x の導手とするとき

$$d(K) = \prod_{x' \in \langle x \rangle} f(x') = n^3$$

をえる[2], [4]. なお, $\mathfrak{z}_j = \begin{cases} 1, & j=0 \\ \eta^{(j-1)}, & j=1,2,3 \end{cases}$ とおいて定義 $d(K) = \det\left(S(\mathfrak{z}_j \mathfrak{z}_k)\right)_{j,k=0,\cdots,3}$ と $S(\eta^2) = S(\eta'^2) = S(\eta''^2) = \frac{1}{4}(3n+1)$ $S(\eta\eta') = S(\eta'\eta'') = S(\eta\eta'') = \frac{1}{4}(-n+1)$ を用いて直接計算することも容易である. ここに S は K/Q に関するスプールを意味する. さらに K の任意の整数 α について α の判別式の仮因子 $Ind\,\alpha = \left[\left\{\prod_{(\sigma)}^{3}(\alpha - \sigma^{(i)}(\alpha))\right\}/d(K)\right]^{\frac{1}{2}}$ を mod.2 で評価しよう. 定義より α を 1 の有理整数倍だけ平行移動しても, あるいは α の共役数に移しても $Ind\,\alpha$ は変らないから α が次の三つの場合を調べれば十分である: (イ) $\alpha \equiv \eta$ mod.2, (ロ) $\alpha \equiv \eta + \eta'$ mod.2, (ハ) $\alpha \equiv \eta + \eta''$ mod.2. まず(イ)の場合はすでに求めたことより $Ind\,\eta = \sqrt{d(\alpha)/d(K)} = 2$ である. さて Gauss の四次剰余の相互法則を用いて $\pi = a + 4i$ について $\chi(2) = \left(\frac{2}{\pi}\right)_4 = i^{-\frac{a}{2}} = -1$ である[4]. よって $\eta^2 \equiv \sum_{x \in H} \zeta^{2x} \equiv \sum_{y \in 2H} \zeta^{y} \equiv \eta''$ mod.2, すなわち $\eta^{(j)2} \equiv \eta^{(j+2)}$ mod.2 j mod.4 が成り立つ. ゆえに(ロ)の場合は $(\eta+\eta')^2 \equiv \eta^2 + \eta'^2$ $\equiv \eta' + \eta''' \equiv 1 + \eta + \eta'$ mod.2 (ハ)の場合は $(\eta+\eta'')^2 \equiv \eta'' + \eta$ mod.2 より

$$Ind(\eta+\eta') \equiv \begin{vmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 1 & 1 & 1 & 0 \\ * & * & * & * \end{vmatrix} \equiv 0 \bmod 2, \quad Ind(\eta+\eta'') \equiv \begin{vmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 \\ * & * & * & * \end{vmatrix} \equiv 0 \bmod 2$$

をえる. したがって体 K の判別式の仮因子 $\mathfrak{d}(K)$ は 2 に等しい. ここで次の補題が必要である. .

補題2. $n(t)=at^2+bt+c$, $a>0$ を有理整係数の多項式とせよ. すべての素数 g について二次合同式 $n(t)\equiv 0 \bmod g^2$ は高々2個の解をもつとする. さらに $a+b$ は偶数, c は奇数のとき t を動かせば $n(t)$ は平方因数を含まない数を無限に多く表す.

証明. いま $x\geqq 1$ について $N(x)=\sum_{\substack{1\leqq t\leqq x\\ n(t)\text{は平方因数をもたない}}} 1$, $M(x)=\sum_{\substack{1\leqq t\leqq x\\ n(t)\text{は平方因数をもつ}}} 1$, さらに任意に固定した素数 g について $M_g(x)=\sum_{\substack{1\leqq t\leqq x\\ g^2\mid n(t)}} 1$ とおく. このとき $N(x)\geqq x-M(x)$, $n(t)$ は奇数であるから十分大きな x について $M(x)\leqq \sum_{3\leqq g\leqq \sqrt{a}x+\frac{b}{2\sqrt{a}}} M_g(x)$ が成り立つ. 条件より $M_g(x)\leqq 2\cdot\frac{x}{g^2}+2$ をえる. よって

$$N(x)\geqq x-\sum_{3\leqq g\leqq \sqrt{a}x+\frac{b}{2\sqrt{a}}}\left(2\cdot\frac{x}{g^2}+2\right)\geqq x-2x\left(\zeta(2)-1-\frac{1}{2^2}\right)+o(x)$$

ここで素数定理を用いた. また $\zeta(2)=\sum_{n=1}^{\infty}\frac{1}{n^2}=\frac{\pi^2}{6}$ より $x\to\infty$ のとき $N(x)\to\infty$ となる. よって補題2の証明は終った.

いま $n(a)=a^2+16$ について $a=4t+1$ とおけるから これは補題2の条件を満足する. 以上をまとめて次の定理をえる.

定理1. 体の判別式の仮因子が2に等しい Q 上四次巡回体 K は無限に多く存在する. このとき K の整数環は中底をもたない.

注意2. とくに $n=f_1f_2$, $f_j=4t+1$, $f_1f_2\equiv -1 \bmod 4$ のとき O_K

は任意の整数 α, β について $1, \alpha, \beta, \alpha^3$ なる形の底をもたない．なお，$\alpha=\eta$, $\beta=\eta'$ と採れば $O_K=\mathbb{Z}[1, \alpha, \alpha^2, \beta]$ は成立する[11].

注意3. 体の判別式の仮因子が3に等しい $\mathbb{Q}$ 上四次巡回体も同様に構成できる[12].

さらに次の結果が従う.

定理2. 体の判別式の仮因子が偶数となり，任意の整数 α β について $\{1, \alpha, \alpha^2, \alpha^3\}$, $\{1, \alpha, \alpha^2, \beta\}$ および $\{1, \alpha, \beta, \alpha^3\}$ のいずれも整数環の底を作らないような $\mathbb{Q}$ 上四次巡回体は無限に多く存在する.

証明. $n=\alpha^2+64$, $\alpha \equiv 1 \bmod 4$ とおけば，n は分解 $n=\pi\bar{\pi}$ $\pi=\alpha+8i$ をもつ．定理1の構成と全く同様に，n が平方因数を含まないとき四次剰余指標 $\chi(*)=\left(\frac{*}{\pi}\right)_4$ で決まる $K_n/\mathbb{Q}$ のガロア群の部分群を H, Gal の $\varphi(n)/4$ 項周期を $\eta=\sum_{\tau\in H}\zeta^{\tau}$ とするとき η を根にもつ $\mathbb{Q}$ 上既約な四次巡回方程式は $n=\prod_{j=1}^{2}\beta_j$ $\beta_j \neq \beta_k\ (j\neq k)$ について

$$X^4-(-1)^2X^3+\frac{3}{8}(-n+1)X-\frac{(-1)^2}{16}\{(2\alpha-3)n+1\}X$$
$$+\frac{1}{256}\{-3n^2+(8\alpha+250)n+1\}=0$$

となる．よって $K=\mathbb{Q}(\eta)$ は $\mathbb{Q}$ 上四次巡回拡大体である．ここに定めた η のパラメータ表示は補題2から整数 α を動かすと

き無限に多くの平方因数を含まない正整数を表す．このときその任意の素因数 p は $\bmod 4$ で 1 と合同でなければならない．一方，Gaussの四次剰余の相互法則の補充法則を再び用いて $\left(\frac{2}{\pi}\right)_4 = i^{\frac{8}{2}} = 1$ をえる．したがって $\eta^2 \equiv \sum_{x\in H} \zeta^{2x} \equiv \sum_{y\in H} \zeta^{y} \equiv \eta \bmod 2$，すなわち $\eta^{(\beta)^2} \equiv \eta^{(\beta)} \bmod 2$, $\beta \bmod 4$ が成り立つ．ゆえに各 $\mathrm{Ind}\,\alpha$ の $\bmod 2$ での評価が次に従う：

$$\mathrm{Ind}\,\eta \equiv \begin{vmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{vmatrix}, \quad \mathrm{Ind}(\eta+\eta') \equiv \begin{vmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 \end{vmatrix}, \quad \mathrm{Ind}(\eta+\eta'') \equiv \begin{vmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 \end{vmatrix}.$$

すなわち各行列についてそれぞれどの三つの行も一次従属である．これで定理2の証明は完了した．

注意4．とくに $n = p_1 p_2 = a^2 + 64$, $\beta = 4b+1$, $b_1 b_2 \equiv -1 \bmod 4$ のとき体 K の判別式の仮因子は4に等しい[11]．

注意5．定理2より円周65等分体 K_{65} の適当な四次部分体 K をとれば $\mathfrak{O}_K$ は雑誌「数学」(1979年7月)の問題31.3.116の(1)に対する一つの肯定的な例を与える．さらに同じ性質をもつ四次巡回体が無数に存在することも示している．

§3．整数環が中底をもつ四次巡回体の例

われわれはこの§で次の命題と系とを与える．

命題1. 素数 $p=a^2+4$, $g\equiv 3 \bmod 4$ に対し方程式

$$X^4-X^3+\frac{1}{8}(-2pg-p+3)X^2+\frac{1}{16}(-2apg+2pg+p-1)X$$
$$+\frac{1}{256}(16pg^2-4p^2g+8apg-4pg+p^2-2p+1)=0$$

の根 η は有理数体 Q 上の四次巡回拡大体 K を生成する. ここに a の符号は $a\equiv 3 \bmod 4$ で決める. このとき数 η の判別式は $p^3g^2\{\frac{1}{16}(pg^2-4g^2-2pg+p)\}^2$ に等しい. さらに $(p-4, 2g-1)$ と 3 とが互いに素ならば K は体の判別式の仮因子をもたない.

系1. 四つの円周等分体 K_{15}, K_{35}, K_{39} および K_{55} の適当な四次巡回部分体の整数環はそれぞれ中底をもつ.

命題1の証明. $n=pg$, $p=a^2+4$, $g\equiv 3 \bmod 4$ とおく. 素数 p は $p=\pi\bar{\pi}$, $\pi=a+2i$, $a\equiv 3 \bmod 4$ なる分解をもつ. K_n/Q のガロア群 G の元 x に対し四次剰余記号 $\chi_p(x)=\left(\frac{x}{\pi}\right)_4$ と平方剰余記号 $\psi_g(x)=\left(\frac{x}{g}\right)$ とで定まる導手 pg の四次指標を χ とする: $\chi=\chi_p\psi_g$. χ で決まる G の部分群を H とおき, H で定まる Gauss の $\varphi(pg)/4$ 項周期を前§と同じく $\eta=\sum_{x\in H}\zeta^x$ とおく. ここに ζ は 1 の一つの原始 pg 乗根である. $\eta+\eta'+\eta''+\eta'''=(-1)^2=1$ である. 次に $\pi=a+2i\equiv 1-2(1-i) \bmod 4$ より $\chi(-1)=\chi_p(-1)\times\psi_g(-1)=(i^{-\frac{a-1}{2}})^2(-1)=1$, したがって $\tau(\chi)\tau(\bar{\chi})=pg$ が成り立つ. さて, 一般 Euler 規準による定義から $\chi^2=\psi_p$ は導手 p の二次指標であり ζ は $\zeta=\zeta_g^r\zeta_p^s$ と分解できる. ここで, s

は $1=p\xi+g\lambda$, ζ_ℓ は1の一つの原始 ℓ 乗根である. したがって $\tau(\chi^2)=\sum_{x\in G}\psi_p(x)\zeta_g^{\nu x}\zeta_p^{\lambda x}=\sum_{\substack{x_2 \bmod g\\ x_2\not\equiv 0 \bmod g}}\zeta_g^{\nu x_2}\sum_{\substack{x_1 \bmod p\\ x_1\not\equiv 0 \bmod p}}\zeta_p^{\lambda x_1}$ が成り立つ.

ここに $x\equiv x_1 \bmod p$, $x\equiv x_2 \bmod g$ とする. よって

$$\tau(\chi^2)=\sum_{\substack{x_2 \bmod g\\ x_2\not\equiv 0 \bmod g}}\zeta_g^{\nu x_2}\,\tau(\psi_p\,|\,\zeta_p^{\lambda})=(-1)\psi_p(\lambda)\tau(\psi_p)$$

をえる. なお $g\lambda\equiv 1 \bmod p$ より $1=\psi_p(g\lambda)=\psi_p(g)\psi_p(\lambda)$, よって $\psi_p(\lambda)=\psi_p(g)$ であるから $\tau(\chi^2)=-\psi_p(g)\sqrt{p}$ が従う. ゆえに

$$\eta\eta'+\eta\eta''+\eta\eta'''+\eta'\eta''+\eta'\eta'''+\eta''\eta'''$$
$$=\frac{1}{16}\{-4\tau(\chi)\tau(\bar\chi)-2\tau(\chi^2)^2+6\}=\frac{1}{8}(-2pg-p+3)$$

が成り立つ.

一方, $\tau(\psi_g)^2=\left(\sqrt{\psi_g(-1)g}\right)^2=-g$, $\tau(\chi)^2=\{\chi_p(g)\psi_g(p)\tau(\chi_p)\tau(\psi_g)\}^2$
$=\{\chi_p(g)\}^2\tau(\chi_p)^2\tau(\psi_g)^2$ を用いて

$$\tau(\chi)^2\tau(\chi^2)+\tau(\bar\chi)^2\tau(\bar\chi^2)=\psi_p(g)\Big[\frac{\tau(\chi_p)^2}{\tau(\psi_p)}\tau(\psi_g)^2\{-\psi_p(g)\tau(\psi_p)\}\tau(\psi_p)$$
$$+\frac{\tau(\bar\chi)^2}{\tau(\bar\psi_p)}\tau(\bar\psi_g)^2\{-\bar\psi_p(g)\tau(\bar\psi_p)\}\tau(\bar\psi_p)\Big]=\pi pg+\bar\pi pg=2apg$$

をえる.

よって $\eta\eta'\eta''+\eta\eta'\eta'''+\eta\eta''\eta'''+\eta'\eta''\eta'''$

$$=\frac{1}{64}\Big[4\{\tau(\chi)^2\tau(\chi^2)+\tau(\bar\chi)^2\tau(\bar\chi^2)\}+2\{-4\tau(\chi)\tau(\bar\chi)-2\tau(\chi^2)^2\}+1\Big]$$
$$=\frac{1}{16}\{2apg+(-2pg-p)+1\},$$

$\eta\eta'\eta''\eta'''$

$$=\frac{1}{256}\Big[-\{\tau(\chi)^4+\tau(\bar\chi)^4\}+\tau(\chi^2)^4+2\tau(\chi)^2\tau(\bar\chi)^2-4\tau(\chi)\tau(\bar\chi)\tau(\chi^2)^2$$
$$+4\{\tau(\chi)^2\tau(\chi^2)+\tau(\bar\chi)^2\tau(\bar\chi^2)\}+\{-4\tau(\chi)\tau(\bar\chi)-2\tau(\chi^2)^2\}+1\Big]$$
$$=\frac{1}{256}\{16pg^2-4p^2g+8apg-4pg+p^2-2p+1\}$$

が成り立つ. ゆえに η を根にもつ方程式は定理に述べたものと一致する. このとき η の判別式を計算すれば $d(\eta)=d(k)$

$\times\{\frac{1}{16}(p^2-4q^2-2p+p)\}^2$ となる．ここに Hasse の導手判別公式を再び用いれば体 K の判別式 $d(K)$ は $\prod_{\chi\in\langle\chi\rangle} f(\chi)=p^3q^2$ に等しい．次に $\zeta=\eta-\eta'$ を根にもつ四次方程式は $X^4-pqX^2+pq^2=0$ となるから ζ の判別式は $d(\zeta)=d(K)\cdot 2^4q^4(p-4)^2$ となる．さて，p, q の条件より $p^2-4q^2-2p+p\equiv 16 \bmod 32$ である．よって $\sqrt{d(\eta)/d(K)}=L$ とおけば L は奇数である．また，$(16L, q)=(p, q)=1$．よって $(p-4, L)$ の任意の約数を l とすれば $16L\equiv 4(-2q+1)\equiv 0 \bmod l$，すなわち $p\equiv 4 \bmod l$, $2q\equiv 1 \bmod l$ かつ l は奇数でなければならない．さらに $\theta=\eta-\eta'$ を根にもつ方程式は $X^4-\frac{1}{2}p(q+1)X^2+pqX+\frac{1}{16}p(p^2-4q^2-2p+p)=0$ となる．θ の判別式 $d(\theta)$ を $\bmod l$ で計算すれば $d(\theta)\equiv 2^4\cdot 3^3 \bmod l$ が成立する．ところが l についての条件より $d(\theta)$ は l で割り切れない．よって体 K の判別式の仮因子は存在しない．命題の証明は完了した．

系1の証明．$\mathrm{Ind}\,\eta=\left|\frac{1}{16}(p^2-4q^2-2p+p)\right|$ より p, q についての不定方程式を解く．$(p-4)q^2-2pq+p=\pm 16$ の解 $\{p, q\}$ は $p-4>0$ より $\{5, 3\}$, $\{5, 7\}$, $\{5, 11\}$ および $\{13, 3\}$ の4組だけである．証明終り．

注意6．体 K を四次巡回体に限るとき O_K が中底をもつ場合は，いまのところ既存の円周5等分体 K_5 と K_{15}, K_{16}, K_{20} の最

大実部分体[6]および系1でみつかった三個の例を加えた七例のみである.

§4. 非巡回, アーベル四次体の整数環

最後にこの§では次の命題が容易に導かれる.

命題2. 整数環が中底をもつようなQ上の非巡回, アーベル四次体は無数に存在する.

証明. $\ell m_1 \equiv 3 \bmod 4$, $\ell m_2 \equiv 2 \bmod 4$ かつ $\ell m_1 m_2$ は平方因数を含まない, に対し四次体 $K = Q(\sqrt{\ell m_1}, \sqrt{\ell m_2})$ を考える. このとき K/Q はガロア群がKleinの四元群に同型な非巡回, アーベル四次拡大である. [7]により O_K の整数基底として $\{1, \sqrt{\ell m_1}, \sqrt{\ell m_2}, \frac{\sqrt{\ell m_2} + \sqrt{m_1 m_2}}{2}\}$ が採れる. いま $\ell = t$, $m_1 = t+2$, $m_2 = 2$ におけば $\eta = \frac{\sqrt{\ell m_2} + \sqrt{m_1 m_2}}{2}$ について $\mathrm{Ind}\,\eta = 1$ をえる. 一方 t は奇数をわたるから $t = 2A+1$ に対し A についての多項式 $(2A+1)(2A+3)$ は補題2の条件を満足する. ゆえにこのような四次体 K は無限に多く存在する. 証明終り.

参考文献

[1] D. S. Dummit; H. Kisilevsky, Indices in cyclic cubic fields.

Number theory and algebra, 29-42, Academic Press, New York,1977.

[2] H. Hasse, Arithmetische Bestimmung von Grundeinheit und Klassenzahl in zyklischen kubischen und biquadratischen Zahlkőrpern, Abh. Deutsch. Akad. Wiss. Berlin, Kl. Math. Nat. Wiss. Nr. 2(1950). Math. Abhandlungen Bd. 3(1975), 289-379.

[3] H. Hasse, Vorlesungen über Zahlentheorie, Springer Verlag, Berlin-Gőttingen-Heiderberg-New York, 1964.

[4] H. Hasse, Zahlbericht, Pysica-Verlag, Würzburg-Wien, 1970.

[5] S. Kuroda; T. Kubota, Number theory(in Japanese), Asakura, Tokyo, 1963.

[6] J. J. Liang, On the integral basis of the maximal real subfield of a cyclotomic field, J. Reine Angew. Math., 286/287(1976), 223-226.

[7] Y. Motoda, On biquadratic fields, Mem. Fac. Sci., Kyushu Univ., Ser. A, 29(1975), 263-268.

[8] M. Onuki, An arithmetic theory of cubic fields(in Japanese), Tokyo Woman's Christian College, Master thesis, 1974, 1-65.

[9] K. Yamamoto; M. Onuki, On Kronecker's theorem about abelian extensions, Sci. Rep. Tokyo Woman's Christian College, No. 35-38(1976), 415-418.

[10] E. von Zylinski, Zur Theorie der ausserwesentlichen Diskriminantenteiler algebraischer Kőrper, Math. Ann., 73(1913), 273-274.

[11] T. Nakahara, On the unessential factor of the discriminant of a cyclic biquadratic field(preprint).

[12] T. Nakahara, On the unessential factor of the discriminant of an abelian biquadratic field(in preparation).